UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DAVID MCCAULEY and JODI WOLFSON, individually, and on behalf of themselves and all others similarly situated, Plaintiffs, v. COMCAST CABLE COMMUNICATIONS, LLC d/b/a Xfinity; CITRIX SYSTEMS, INC. Defendants.	Case No. 2:24-cv-280 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs David McCauley and Jodi Wolfson ("Plaintiffs"), on behalf of themselves and all others similarly situated ("Class Members"), file this Class Action Complaint ("Complaint") against Defendants Comcast Cable Communications, LLC d/b/a Xfinity ("Comcast") and Citrix Systems, Inc. ("Citrix") (collectively, "Defendants"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to safeguard and secure the personally identifiable information ("PII") of approximately 35.8 million individuals, including Plaintiffs. The individuals affected are former and current customers of Comcast.

2. The data reportedly exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. As a result of Defendants' negligence, between approximately October 16, 2023, and October 19, 2023, cybercriminals were able to gain access to Comcast's customer and access this sensitive and valuable PII (the "Data Breach").

3. According to information provided by Comcast to customers, information disclosed in the Data Breach includes, but is not limited to, usernames and hashed passwords, names, contact information, last four digits of Social Security numbers, dates of birth, and/or secret questions and answers (collectively the "PII").[1]

4. Comcast is a division of Comcast Corporation that provides cable television, internet, telephone, wireless, and other technology services to customers.[2]

5. According to a notice letter sent by Comcast to victims of the data breach (the "Notice Letter"), including Plaintiffs, "[o]n October 10, 2023, one of Xfinity's software providers, [Defendant] Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide."[3] Prior to Comcast's "mitigation," between approximately October 16 and October 19, 2023, there was cybersecurity incident resulting in unauthorized access to some of Comcast's internal systems.[4]

6. Comcast detected that the Data Breach occurred on or about October 25, 2023.[5] On approximately November 16, 2023, Comcast determined that "information" was likely acquired, and on approximately December 6, 2023, it determined the extent of that information, as listed above.[6]

---

[1] *See Notice to Customers of Data Security Incident*, XFINITY, https://assets.xfinity.com/assets/dotcom/learn/Notice%20To%20Customers%20of%20Data%20Security%20Incident.pdf?cjdata=MXxOfDB8WXww&cjevent=3327cd5bae4511ee82aec5330a82b824&cmp=aff__100357191 (last visited Jan. 16, 2024) ("Notice Letter").

[2] *Xfinity*, Comcast, https://corporate.comcast.com/company/xfinity (last visited Jan. 16, 2024).

[3] Notice Letter, *supra* n. 2.

[4] *Id.*

[5] *Notice to Customers of Data Security Incident*, BUSINESSWIRE (Dec. 18, 2023, 4:30 PM), https://www.businesswire.com/news/home/20231218979935/en/Notice-To-Customers-of-Data-Security-Incident.

[6] Notice Letter, *supra* n. 2.

7. Despite learning of the Data Breach nearly two months beforehand, Comcast did not begin alerting Plaintiffs and other victims of the Data Breach until approximately December 18, 2023.[7]

8. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial information in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, and using Class members' PII to target other phishing and hacking intrusions.

9. Plaintiffs and Class members relied on Comcast (and, therefore, on Citrix) to keep their PII confidential and only to make authorized disclosures of this PII, which Defendants failed to do.

10. Defendants owed a non-delegable duty to Plaintiffs and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PII from unauthorized access and disclosure.

11. As a result of Defendants' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiffs and Class members as a result. Plaintiffs bring this action on behalf of themselves and all persons whose PII was exposed as a result of the Data Breach.

---

[7] *See Notice to Customers of Data Security Incident*, *supra* n. 6.

12. Plaintiffs and Class members are now at a significantly increased risk of fraud, identity theft, intrusion of their privacy, and similar forms of criminal mischief, which risk may last for the rest of their lives. Consequently, Plaintiffs and Class members must devote substantially more time, money, and energy protecting themselves now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs seek remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendants' data security system, future annual audits, and adequate credit monitoring services funded by Defendant.

14. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, negligence *per se*, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

A. Plaintiffs

15. Plaintiff David McCauley is an adult individual who is a citizen and resident of the Commonwealth of Virginia. On December 26, 2023, Plaintiff McCauley received a letter from Comcast notifying him that his PII was among the information accessed by cybercriminals in the Data Breach.

16. Since Plaintiff McCauley is, or has been a customer of Comcast, Plaintiff McCauley's PII was maintained within Comcast's networks and servers.

17. Plaintiff Jodi Wolfson is an adult individual who is a citizen and resident of the State of New Jersey. On December 20, 2023, Plaintiff Wolfson received a letter from Comcast

notifying her that her PII was among the information accessed by cybercriminals in the Data Breach.

18. Since Plaintiff Wolfson is, or has been a customer of Comcast, Plaintiff Wolfson's PII was maintained within Comcast's networks and servers.

19. Had Plaintiffs known that Comcast would not adequately protect their and Class members' PII, they would not have paid for and received services from Comcast or any of its affiliates and would not have provided their PII to Comcast or any of its affiliates. This expectation and mutual understanding extended to software providers, like Citrix, that Comcast uses for business purposes.

20. Plaintiffs and Class members are, or were, customers of Comcast. To obtain products and/or services, consumers like Plaintiffs and Class members are required to provide Comcast directly with sensitive PII. In the regular course of its business, Comcast collects, stores, and maintains the PII it receives from consumers who utilize Comcast's products and or/services.

21. By creating and maintaining massive repositories of PII, Comcast has provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

22. In response and as a result of the Data Breach, Plaintiffs and Class members have spent significant time and effort researching the Data Breach and reviewing and monitoring their accounts for fraudulent activity.

23. Plaintiff and Class members suffered damages as a result of the failures of Defendants to adequately protect the sensitive information entrusted to it, including, without limitation, experiencing fraud or attempted fraud, time related to monitoring their accounts for fraudulent activity, exposure to increased and imminent risk of fraud and identity theft, the loss in value of their personal information, and other economic and non-economic harm. Plaintiff and

Class members will now be forced to expend additional time to review their credit reports and monitor their accounts for fraud or identity theft.

24. As a result of the Data Breach, Plaintiff and Class members have been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such risk is certainly real and impending and is not speculative given the highly sensitive nature of the PII compromised by the Data Breach.

B. **Defendants**

25. Defendant Comcast Cable Communications, LLC, d/b/a Xfinity, is a Delaware limited liability company with its principal place of business located at Comcast Center, 1701 JFK Boulevard, Philadelphia, Pennsylvania, 19103. Comcast is a cable and internet service provider that operates nationwide, including in the Commonwealth of Pennsylvania. Comcast is registered to do business with the Pennsylvania Department of State.

26. Comcast is "a leading provider of broadband, video, voice, wireless, and other services to residential customers in the United States; [it] also provide[s] these and other services to business customers and sell[s] advertising."[8] According to a recent earnings release, Comcast has more than 32 million broadband customers.[9] Xfinity provides nationwide coverage through a

[8] *Id.*

[9] *See* The Associated Press, *See Nearly 35.9 million affected by Xfinity data breach: filings*, WWLP NEWS (Dec. 19, 2023), https://www.wwlp.com/news/national/nearly-35-9-million-affected-by-xfinity-data-breach-filings/.

broad range of WiFi options, and it claims to be "the largest internet provider in the U.S."[10] Xfinity Mobile has "reached six million customer lines in six years, and growing."[11]

27. Defendant Citrix Systems, Inc. is a Delaware corporation with its principal place of business located at 851 Cypress Creek Road, Fort Lauderdale, Florida 33309.

28. Citrix is a multinational cloud computing and virtualization technology company that provides server, application and desktop virtualization, networking, software as a service (SaaS), and cloud computing technologies. Citrix is registered to do business with the Pennsylvania Department of State.

JURISDICTION AND VENUE

29. This Court has subject matter jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

30. This Court has general personal jurisdiction over Defendants because each are registered to do business with the Pennsylvania Department of State. Further, Comcast is headquartered and has their principal place of business in the Eastern District of Pennsylvania.

31. This Court has general personal jurisdiction over Defendants because each routinely conducts business in the Commonwealth of Pennsylvania, has sufficient minimum contacts in the Commonwealth of Pennsylvania, has intentionally availed themselves of this jurisdiction by marketing and/or selling products and/or services and/or by accepting and

[10] *Connectivity & Platforms*, COMCAST, https://corporate.comcast.com/company/connectivity-platforms (last visited Jan. 16, 2024).

[11] *Wireless*, COMCAST, https://corporate.comcast.com/company/xfinity/wireless (last visited Jan. 16, 2024).

processing payments for those products and/or services within the Commonwealth of Pennsylvania.

32. Venue in proper in this District pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events that gave rise to Plaintiffs' claims occurred within this District.

FACTUAL ALLEGATIONS

A. The Data Breach and Notice Letter

33. On October 10, 2023, Citrix, one of Xfinity's software providers, announced a vulnerability in one of its network hardware products used by Xfinity, and issued a patch to address the vulnerability.[12]

34. While Comcast claims that it "promptly patched and mitigated [its] systems[,]" that is not so; Comcast didn't patch its network until between approximately October 16 and October 19, failing to secure its system for a week after it learned of the vulnerability.[13]

35. On or about October 25, 2023, Comcast determined that between approximately October 16 and October 19, 2023, prior to its purported patch and mitigation, there was "unauthorized access to its internal systems that was concluded to be a result of this vulnerability."[14]

---

[12] Notice Letter, *supra* n. 2; *see Understanding Patches and Software Updates*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Feb. 23, 2023), https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates ("Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced security features.").

[13] *See* Notice Letter, *supra* n. 2.

[14] *Notice to Customers of Data Security Incident*, *supra* n. 6.

36. On or about November 16, 2023, Comcast determined that "information" was likely acquired, and on or about December 6, 2023, it determined the extent of that information, as described in the Notice Letter as: "usernames and hashed passwords[,] . . . . names, contact information, last four digits of Social Security numbers, dates of birth, and/or secret questions and answers."[15]

37. While Comcast has not confirmed the name of the vulnerability in Citrix's software, it has been "dubbed 'CitrixBleed,' [and] has also been linked to hacks targeting the Industrial and Commercial Bank of China's New York arm and a Boeing subsidiary, among others."[16]

38. Comcast also has not confirmed the name of the cybercriminal group responsible for this Data Breach, but news organizations have reported that "[o]ne of the threat actors is believed to be the Russia-linked Lockbit ransomware gang, which has already claimed responsibility for several large-scale breaches believed to be associated with CitrixBleed."[17]

39. According to the breach report Comcast submitted to the Maine Attorney General, the Data Breach affected up to 35.8 million individuals.[18]

40. The Notice Letter Comcast provided to victims is glaringly deficient.[19]

---

[15] Notice Letter, *supra* n. 2 ("Password hashing uses an algorithm to turn your password into a short string of different numbers and letters for security purposes.").

[16] Megan Cerullo, *Xfinity hack affects nearly 36 million customers. Here's what to know.*, CBS NEWS (Dec. 20, 2023, 10:39 AM), https://www.cbsnews.com/news/xfinity-hack-customers-usernames-passwords/.

[17] Carly Page, *Hackers are exploiting 'CitrixBleed' bug in the latest wave of mass cyberattacks*, TECHCRUNCH+ (Nov. 14, 2023), https://techcrunch.com/2023/11/14/citrix-bleed-critical-bug-ransomware-mass-cyberattacks/.

[18] *Data Breach Entry*, *supra* n. 1.

[19] *See* Notice Letter, *supra* n. 2.

41. While Comcast began notifying affected individuals on or about December 18, 2023, Comcast waited at least 62 days from the date it learned of the Data Breach to directly notify some affected individuals, as Plaintiff McCauley was not notified until December 26, 2023.

42. To date, Comcast has not disclosed crucial information, including, but not limited to: how many of its customers were affected by the Data Breach; how the cybercriminals were able to exploit vulnerabilities in Defendants' IT security systems; the steps taken by Comcast when it allegedly "promptly patched and mitigated" its systems; the identity of the hacking group responsible for the Data Breach, or the specific measures, if any, Comcast has since taken to enhance its security safeguards.

43. While Comcast has not disclosed the exact data obtained in the Data Breach, its Notice Letter informed Plaintiffs and Class members that the data likely consists of PII including, but not limited to, usernames and hashed passwords, names, contact information, last four digits of Social Security numbers, dates of birth, and/or secret questions and answers.[20]

44. Comcast recognizes the long-term risks to Plaintiffs and Class members resulting from the Data Breach, as evidenced by their recommendation in the Notice to "remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports."[21]

45. Comcast also provides on its website "Xfinity Privacy Commitments" that recognizes its customers' "essential" right to privacy and its belief that "strong cybersecurity is essential to privacy."[22]

---

[20] *Id.*
[21] *Id.*

[22] *Xfinity Privacy Commitments*, COMCAST, https://corporate.comcast.com/privacy (last updated Jan. 2023).

46. Yet, despite the ongoing and long-term risks for financial fraud and identity theft for victims of the Data Breach, Comcast does not provide any identity protection services for the affected individuals.[23]

47. While Comcast offers free of charge security freezes or fraud alerts, it puts the burden on Data Breach victims to sign up for these services, and it also recognizes that these have substantial drawbacks, including "prevent[ing] the timely approval of . . . requests . . . for new loans, credit mortgages, employment, housing, or other services[,]" and "delay[ing] your ability to obtain credit while the agency verifies your identity."[24]

48. Comcast's systems hacked by cybercriminals contained Plaintiffs' and Class members' PII that was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

49. Plaintiffs and Class members provided their PII to Comcast, either directly or indirectly, with the reasonable expectation and mutual understanding that Comcast would comply with its obligation to keep such information confidential and secure from unauthorized access.

50. Comcast also benefited directly from the PII provided by Plaintiffs and Class members. As stated in Comcast's publicly available Privacy Policy, Comcast "use[s] the information [it] collect[s] to provide [its] Services and communicate with [customers]. [It] also use[s] it to improve [its] Services, develop new products and services, give recommendations, deliver personalized consumer experiences . . . , investigate theft and other illegal activities, and to ensure a secure online environment."[25]

---

[23] Notice Letter, *supra* n. 2.

[24] *Id.*

[25] *Our Privacy Policy*, XFINITY, https://www.xfinity.com/privacy/policy#info-collection (last updated Jan. 1, 2024).

51. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII, Comcast assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiffs' and Class members' PII from unauthorized disclosure.

B. Defendants Knew That Criminals Target PII

52. At all relevant times, Defendants knew, or should have known, Plaintiffs' and all other Class members' PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

53. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

54. Lockbit, the cybercriminal group who reportedly took responsibility for several large-scale breaches believed to be associated with CitrixBleed, was the subject of a June 2023 Cybersecurity Advisory by the Cybersecurity and Infrastructure Security Agency – months prior to the Data Breach.[26] This advisory "detail[ed] observed activity in LockBit ransomware incidents and provid[ed] recommended mitigations to enable network defenders to proactively improve their organization's defenses against this ransomware operation."[27]

---

[26] *Understanding Ransomware Threat Actors: LockBit*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Jun. 14, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a ("In 2022, LockBit was the most deployed ransomware variant across the world and continues to be prolific in 2023.").

[27] *Id.*

55. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[28]

56. As a result of the notoriety of cyberattacks on systems like Defendants, several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

57. In light of the high-profile data breaches and a wealth of relevant guidance and news reports at Defendants' disposal, Defendants knew or should have known that its electronic records and customers' PII would be targeted by cybercriminals.

58. These data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to improve the security of their systems and engage in stronger, more comprehensive cybersecurity practices.

59. PII is a valuable property right.[29] The value of PII as a commodity is measurable.[30] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

---

[28] *See, e.g., Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited Jan. 16, 2024).

[29] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[30] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[31] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[32] In fact, it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

60. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, and other PII directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

61. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[33]

62. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[31] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[32] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[33] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

63. Therefore, Defendants clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII stored in its unprotected files and the massive amount of PII it maintains.

C. Theft of PII has Grave and Lasting Consequences for Victims

64. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[34]

65. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[35] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[36]

---

[34] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[35] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[36] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited Jan. 16, 2024).

66. Indeed, Attorney Steven Weisman, the editor of Scamicide.com, says that hackers can easily use the last four digits of people's Social Security numbers, as was exposed in the Data Breach, to determine the first five digits themselves, since "they relate to where you live and where your card was issued."[37]

67. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit.

68. Indeed, Plaintiffs have already begun the long and arduous process of preventing further harm and injury resulting from the Data Breach. Plaintiff McCauley has spent time and money enrolling in identity theft protection services, which informed him that his Social Security information was on the "dark web." Plaintiff Wolfson has spent time coordinating services and protective measures with her bank, her phone number was changed without her consent, and a fraudulent Amazon account was opened in her name. Plaintiffs have both suffered emotionally over the stress resulting from the Data Breach.

69. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[38] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[37] Alanna Flood & Amy Phillips, *Social Security numbers of some Xfinity customers vulnerable in latest data breach: What to know*, THE HILL (Dec. 30, 2023), https://thehill.com/homenews/4381585-social-security-numbers-of-some-xfinity-customers-vulnerable-in-latest-data-breach-what-to-know/.

[38] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

70. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[39]

71. There may be a time lag between when PII is stolen and when it is used.[40] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

72. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other PII directly on various Internet websites making the information publicly available.

73. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your

---

[39] *Id.* at 2, 9.

[40] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[41] U.S. GOV'T ACCOUNTABILITY OFF., *supra* n. 41 at 29 (emphasis added).

name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[42]

74. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[43]

75. Plaintiffs and Class members must vigilantly monitor their financial accounts, as well as the accounts of their family members, for many years to come.

76. It is within this context that Plaintiffs and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

D. **Damages Sustained by Plaintiffs and the Other Class Members**

77. Plaintiffs and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft and medical

[42] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[43] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited Jan. 16, 2024).

identity theft they face and will continue to face; and (v) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

78. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

79. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

> All persons in the United States whose PII was accessed in the Data Breach by unauthorized persons, including all persons who were sent a notice of the Data Breach (the "Class").

80. Plaintiffs reserve the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

81. Plaintiffs are members of the Class.

82. Excluded from the Class are Defendants, and their affiliates, parents, subsidiaries, officers, agents, and directors, and the judge(s) presiding over this matter and the clerks of said judge(s).

83. This action seeks both injunctive relief and damages.

84. Plaintiffs and the Class satisfy the requirements for class certification for the following reasons:

85. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. While the exact number of Class members is unknown at this time, Class members are readily identifiable in Defendants' records, which will be a subject of discovery. Upon information and belief, there are millions of Class members in the Class.

86. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

c. Whether Defendants owed a duty to Plaintiffs and Class members to safeguard their PII;

d. Whether Defendants breached its duty to Plaintiffs and Class members to safeguard their PII;

e. Whether Defendants failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class members;

f. Whether Plaintiffs' and Class members' PII was compromised in the Data Breach;

g. Whether Plaintiffs and Class members are entitled to injunctive relief; and

h. Whether Plaintiffs and Class members are entitled to damages as a result of Defendants' conduct.

87. **Typicality.** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs and Class members all had their PII stolen in the Data Breach. Plaintiffs' grievances, like the proposed Class members' grievances, all arise out of the same business practices and course of conduct by Caesar.

88. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent the Class on whose behalf this action is prosecuted. Their interests do not conflict with the interests of the Class.

89. Plaintiffs and their chosen attorneys are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, they have been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. Plaintiffs' counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class members. Finally, Plaintiffs' counsel possess the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

90. **Predominance.** The common issues identified above arising from Defendants' conduct predominate over any issues affecting only individual Class members. The common issues hinge on Defendants' common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

91. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class members can obtain the most compensation possible.

92. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendants has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class members and as to Defendants.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only customers of Comcast, the legal and factual issues

are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class members can be identified from Comcast's records, such that direct notice to the Class members would be appropriate.

93. **Injunctive relief.** Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By All Plaintiffs Against All Defendants)

94. Plaintiffs and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

95. As a condition of receiving Comcast's products and/or services, Plaintiffs and Class members were required to and did provide Comcast with their PII.

96. By collecting and storing their PII and using it for commercial gain, at all times relevant, Comcast owed a duty to Plaintiffs and all other Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

97. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with statutory and industry standards and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

98. Defendants knew the risks of collecting and storing Plaintiffs' and all other Class members' PII and the importance of maintaining secure systems in the software they provide. Defendants knew of the many data breaches that targeted companies that store PII in recent years.

99. Given the nature of Defendants' businesses, the sensitivity and value of the PII they maintain, and the resources at its disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

100. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them -- including Plaintiffs' and Class members' PII.

101. Plaintiffs and Class members are a well-defined, foreseeable, and probable group of customers that Defendants was aware, or should have been aware, could be injured by inadequate data security measures.

102. Plaintiffs and Class members have no ability to protect their PII that was or remains in Defendants' possession.

103. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

104. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII would not have been compromised.

105. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect Plaintiffs' and Class members' PII and failing to provide them with timely notice that their PII had been compromised.

106. Neither Plaintiffs nor Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

107. By failing to provide timely and complete notification of the Data Breach to Plaintiffs and Class members, Defendants prevented them from proactively taking steps to secure their PII and mitigate the associated threats.

108. As a result of Defendants' above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and all other Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE *PER SE*
(By All Plaintiffs Against All Defendants)

109. Plaintiffs and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

110. Defendants had duties by statute to ensure that all information they collected and stored was secure, and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiffs' and Class members' PII.

111. Defendants' duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendant, of failing to employ reasonable measures to protect and secure PII.

112. The FTC has published numerous guides for businesses, which highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[44]

113. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

[44] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

unfair act or practice prohibited by Section 5 of the FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendants must take to meet their data security obligations, and effectively put Defendants on notice of these standards.

114. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and all Class members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiffs and other Class members.

115. Defendants' violation of these federal and state laws constitutes negligence *per se*.

116. Plaintiffs and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

117. The harm occurring as a result of the Data Breach is the type of harm against which Section 5 of the FTCA was intended to guard against.

118. It was reasonably foreseeable to Defendants that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class members' PII to unauthorized individuals.

119. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' violation of Section 5 of the FTCA. Plaintiffs and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity

theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

120. Defendants' violation of the FTCA and state data security statutes constitute negligence *per se* for purposes of establishing the duty and breach elements of Plaintiffs' negligence claim. Those statutes were designed to protect a group to which Plaintiffs belong and to prevent the type of harm that resulted from the Data Breach.

121. Defendants owed a duty of care to the Plaintiffs and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

122. It was foreseeable that Defendants' failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Class were reasonably foreseeable.

123. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card

statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF IMPLIED CONTRACT
(By All Plaintiffs Against Comcast)

124. Plaintiffs and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

125. In connection with receiving products and/or services, Plaintiffs and all other Class members entered into implied contracts with Comcast.

126. When Plaintiffs and Class members paid money and provided their PII to Comcast, either directly or indirectly, as a pre-condition and in exchange for goods or services, they entered into implied contracts with Defendant.

127. Pursuant to these implied contracts, in exchange for the consideration and PII provided by Plaintiffs and Class members, Comcast agreed to, among other things, and Plaintiffs understood that Comcast would: (1) provide products and/or services to Plaintiffs and Class members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

128. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and Comcast, on the other hand. Indeed, as set forth *supra*, Comcast recognized its duty to provide adequate data security and ensure the privacy of its consumers' PII with its practice of providing a privacy policy on its website.

129. Plaintiffs and Class members performed their obligations under the implied contract when they provided Comcast with their PII and paid for the services from Defendant.

130. Plaintiffs and Class members would not have entrusted their PII to Comcast in the absence of such an implied contract.

131. Had Plaintiffs and Class members known that Comcast would not adequately protect its customers' and former customers' PII, they would not have received services from Defendant.

132. Comcast breached its obligations under its implied contracts with Plaintiffs and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

133. Comcast's breach of their obligations of its implied contracts with Plaintiffs and Class members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

134. Plaintiffs and all other Class members were suffered by Comcast's breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; (vi) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT
(By All Plaintiffs Against Comcast)

135. Plaintiffs and Class members reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

136. This claim is pleaded in the alternative to the breach of implied contract claim.

137. Plaintiffs and Class members conferred a monetary benefit upon Comcast in the forms of (1) monies paid for services, and (2) the provision of their valuable PII. Indeed, upon acquiring the PII, Comcast was then able to charge money for its services and utilize the PII to "improve [its] Services, develop new products and services, give recommendations, [and] deliver personalized consumer experiences[.]"[45] The PII was thus used to facilitate payment and generate additional revenue for Comcast.

138. Comcast accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class members. Comcast profited from these transactions and used the PII of Plaintiffs and Class members for business purposes.

139. Upon information and belief, Comcast, like most other corporate entities, fund their data security measures entirely from their general revenue, which includes money paid by Plaintiffs and Class members.

140. As such, a portion of the payments made by or on behalf of Plaintiffs and Class members is or should have been used to provide a reasonable level of data security.

141. Comcast enriched itself by saving the costs it reasonably should have expended on data security measures to secure its customers' PII.

[45] *Our Privacy Policy*, *supra* n. 28.

142. Instead of providing a reasonable level of security that would have prevented the Data Breach, Comcast calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing less expensive and less effective security measures.

143. As a direct and proximate result of Comcast's failure to provide the requisite security, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

144. Comcast should not be permitted to retain the money belonging to Plaintiffs and Class members because Comcast failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

145. Comcast should be compelled to provide for the benefit of Plaintiffs and Class members all unlawful proceeds received by it as a result of its conduct and the resulting Data Breach alleged herein.

COUNT V
DECLARATORY AND INJUNCTIVE RELIEF
U.S.C. §§ 2201, *et seq.*
(By All Plaintiffs Against All Defendants)

146. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

147. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the statutes described in this Complaint.

148. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and statutory duties to reasonably safeguard its customers' and its clients' customers' sensitive personal information and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches. Plaintiff alleges that Defendants' data security practices remain inadequate.

149. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their sensitive personal information and remain at imminent risk that further compromises of their personal information will occur in the future.

150. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants continue to owe a legal duty to secure customers' sensitive personal information, to timely notify customers of any data breach, and to establish and implement data security measures that are adequate to secure customers' sensitive personal information.

151. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' sensitive personal information.

152. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, for which they lack an adequate legal remedy. The threat of another data breach is real, immediate, and substantial. If another data breach at Defendants occur, Plaintiff and Class Members will not have an adequate remedy at law because not all of the resulting injuries are readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

153. The hardship to Plaintiff and Class Members if an injunction does not issue greatly exceeds the hardship to Defendants if an injunction is issued. If another data breach occurs,

Plaintiff and Class Members will likely be subjected to substantial risk of identity theft and other damages. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants has a pre-existing legal obligation to employ such measures.

154. Issuance of the requested injunction will serve the public interest by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and the millions of customers whose confidential information would be further compromised.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in his favor and against Defendants as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiffs as Class representatives and the undersigned counsel as Class Counsel;

B. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiffs and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiffs and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiffs and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: January 21, 2024

Respectfully submitted,

/s/ Anthony M. Christina

Todd S. Garber (*pro hac vice f*orthcoming)
Andrew C. White (*pro hac vice f*orthcoming)
FINKELSTEIN, BLANKINSHIP FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Paul M. Sod (*pro hac vice f*orthcoming)
337R Central Avenue
Lawrence, New York 11559
Tel: (516) 295-0707
paulmsod@gmail.com

Christian Levis (*pro hac vice f*orthcoming)
Amanda G. Fiorilla (*pro hac vice f*orthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, New York 10601
Tel: (914) 997-0500
clevis@lowey.com
afiorilla@lowey.com

Anthony M. Christina
PA ID# 322528
LOWEY DANNENBERG, P.C.
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, Pennsylvania 19428
Tel: (215) 399-4770
achristina@lowey.com

Attorneys for Plaintiffs and the Proposed Class